BANGALORE ELECTRICITY SUPPLY COMPANY LIMITED

Corporate Office, K RCircle,

Bengaluru – 560 001

Address : **O/o The General Manager (DAS)**
BICC-1, 2nd
Sector, 24th main,
17th Cross, HSR Layout,
Bengaluru- 560102.
Cell :+91-9448279010

Email Id : gmdas@bescom.co.in

Enquiry no: BESCOM/2026-27/EL/WORK_INDENT108

TENDER FOR "Automation of NON DAS Feeders in BMAZ Area BESCOM"

SECTION 6F

Cyber Security requirements for Automation of NON-DAS feeders in BMAZ area BESCOM.

1. Preamble

This Annexure defines the mandatory cybersecurity requirements applicable to all equipment, software, firmware, communication infrastructure, engineering tools, and services supplied under the DAS Expansion Project.

These requirements form part of a new specification/upgrade. Formal cybersecurity conformance testing, third-party certification, or audit against the referenced standards may not have been carried out at earlier stages; however, under this tender, compliance shall be demonstrated through documented technical capability, conformance statements, and where required, independent validation.

The requirements shall apply to:

- RMUs, MFMs
- Protection relays
- RTUs
- Communication gateways
- Engineering access interfaces (USB/Serial)
- Serial/IP communication infrastructure
- Control centre/DAS/SCADA integrations
- Supply chain and lifecycle processes

Non-compliance with mandatory clauses may render the bid non-responsive.

2. Applicable IS/IEC/IEEE Cybersecurity Standards for DAS & OT Systems

For Distribution Automation Systems, Substation Automation, and OT environments, the following standards are typically referenced for defining cybersecurity requirements:

- IEC 62443 (Security for Industrial Automation and Control Systems – IACS)
- IEC 62351 (Power systems management and associated information exchange – Data and communications security)
- IEEE 1686 (Cybersecurity capabilities for Intelligent Electronic Devices – IEDs)
- Cyber Security Guidelines for Power Sector issued by Central Electricity Authority
- Guidelines and directions issued by Indian Computer Emergency Response Team

These standards collectively address:

- Secure architecture
- Communication security
- Access control
- System hardening
- Cybersecurity management practices in power sector OT deployments

It is also suggested to follow the complete NCIIPC National Cybersecurity Reference Framework (NCRF) Version 1.0 and Compendium of Guidelines, Standards & Frameworks.

3. Governance, ISMS, and Service Management Standards.

Organisations, specifically regulated and critical sector entities, shall obtain guidance from:

- ISO/IEC 38500 (Governance of IT)

- ISO/IEC 27014 (Information security governance)
- COBIT framework
- IS/ISO/IEC 20000 family (Service Management System – SMS)
- IS/ISO/IEC 27000 family (Information Security Management System – ISMS)
- ISO 27013 (Concurrent implementation of ISO 27001 and ISO 20000-1)
- ISO 22301 (Business Continuity)

Sector-specific standards include:

- ISO 27019 (Power sector information security controls)
- IEC 62443
- IEC 60870

4. Detailed IEC 62443 Structure (As Referenced)

The IEC 62443 series is organized into four parts:

Part 1 – General

1.1 (TS): Terminology, concepts and models

Part 2 – Policies and Procedures

2-1: Establishing an IACS security program
2-3 (TR): Patch management in the IACS environment
2-4: Security program requirements for IACS service providers

Part 3 – System Level

3-1: Security technologies for IACS
3-2: Security risk assessment for system design
3-3: System security requirements and security levels

Part 4 – Component Level

4-1: Secure product development lifecycle requirements
4-2: Technical security requirements for IACS components

5. Protocol-Specific Cybersecurity Requirements

5.1 MODBUS (RS-232 / RS-485)

MODBUS (serial) does not inherently provide encryption or authentication mechanisms.

Security in such deployments shall be achieved through:

- Physical access control to field devices
- Network segmentation and isolation
- Use of secure gateways or protocol converters with authentication and traffic filtering
- Controlled engineering access procedures
- Physical and logical protection of serial ports
- Role-based control of engineering access via USB/serial

Where MODBUS TCP is implemented, compliance shall align with:

- IEC 62351-3
- IEC 62443-3-3
- IEC 62443-4-2
- MODBUS TCP Security

5.2 DNP 3.0 (Serial and IP)

Security mechanisms shall comply with IEC 62351-5 and IEC 62351-3, including:

- Implementation of DNP3 Secure Authentication (latest supported version)
- Secure authentication for control commands
- Message integrity protection
- Replay protection
- Strong device authentication
- Secure key management

Security implementation shall consider device capability and system-level configuration.

5.3 IEC 60870-5-101 / 103 / 104

IEC 101 / 103 (Serial)

These rely primarily on deployment-level controls including:

- Network isolation
- Controlled access
- IEC 60870-5-7
- IEC 62351-5

IEC 104 (IP-Based)

May be secured using TLS-based communication mechanisms as described in IEC 62351-3.

Shall include:

- TLS encryption
- Authentication of control commands
- Session integrity
- Protection against message tampering

6. Device-Level Cybersecurity Test Requirements

OEMs must demonstrate that devices such as SPBs, RMUs, MFMs, protection relays, FRTUs, LRCs, and LBSs support:

6.1 Access Control

- Role-Based Access Control (RBAC)
- Unique user credentials
- Password policy enforcement
- Account lockout mechanisms

6.2 Authentication

- Secure local login
- Secure remote login
- Certificate/key-based authentication (where applicable)

6.3 Secure Communication

- Encrypted communication for IP-based protocols
- Secure protocol variants (DNP3-SA, IEC 62351-compliant implementations)

6.4 Interface & Port Security

- Ability to disable unused ports/services
- Logging of engineering access via USB/serial

6.5 Logging & Audit

- Logging of security-relevant events (logins, configuration changes, firmware updates)
- Time-synchronized logs
- Exportable audit logs

6.6 System Hardening

- Removal of default credentials
- Secure, integrity-protected firmware update mechanisms

6.7 Cyber Resilience

- Resistance to unauthorized access attempts
- Robust handling of malformed protocol traffic
- Stable behaviour under denial-of-service conditions

7. System-Level Cybersecurity Requirements

System architecture shall include:

- Segmentation between OT and IT networks
- Firewalls and secure gateways at protocol transition points
- Centralized authentication and access governance
- Controlled remote access using VPN with MFA
- Defined patch and vulnerability management processes
- Integration of logs with centralized monitoring/SOC platforms

Cybersecurity testing and verification shall cover:

- Secure communication channels for IP-based protocols
- Network segmentation (zones and conduits concept)
- Firewall and gateway enforcement
- Logging and monitoring integration
- Basic resilience considerations against unauthorized access or network misuse

8. Recommended Cybersecurity Conformance / Certification Alignment

Vendors/OEMs are expected to align with:

- IEC 62443-based system security level assessment
- IEC 62351 protocol security conformance testing
- IEEE 1686 capability verification for IEDs
- IEC 62443-4-1 (Secure Product Development Lifecycle)
- IEC 62443-4-2 (Technical Security Requirements for Components)
- IEC 62443-3-3 (System Security Requirements)
- Independent cybersecurity testing through accredited laboratories
- Device-level vulnerability assessment and penetration testing
- Utility-specific cybersecurity audit frameworks

9. Assurance Documents to be Submitted by OEMs

Utilities may request submission of the following, which shall be mandatory under this tender:

- OEM cybersecurity capability statements
- Cybersecurity architecture or design notes
- Protocol capability documentation
- Secure configuration and hardening guidelines
- Factory Acceptance Test (FAT) reports (as per agreed scope)
- Vendor cybersecurity policy
- Vulnerability handling process
- Declaration of conformity to relevant IEC 62443 requirements
- IEC 62351 compliance statement
- IEEE 1686 capability statement
- Secure Development Lifecycle (SDL) documentation
- Cybersecurity test reports (VA/PT and protocol security testing)
- Firmware integrity and secure update process description
- Hardening guide and list of open ports/services
- Patch management and vulnerability disclosure policy
- Software Bill of Materials (SBOM), where available

Formal third-party cybersecurity certificates shall be furnished where such certification has been completed or contractually mandated.

10. Cybersecurity Validation

Should BESCOM require specific cybersecurity validation, audit, or certification as part of the project execution scope, the same shall be undertaken subject to agreed scope and compliance requirements.

CYBER SECURITY TEST CASE TEMPLATE

(Factory Acceptance Test – FAT / Site Acceptance Test – SAT)

Project: Automation of NON-DAS feeders in BMAZ area – BESCOM
Equipment Type: RMU / MFM / Protection Relay / RTU
OEM:
Model No.:
Firmware Version:
Test Location: FAT / SAT
Test Date:
Tested By:
Witnessed By (BESCOM):

Testing shall align with the security requirements of IEC 62443, IEC 62351 and IEEE 1686 wherever applicable.

SECTION A – ACCESS CONTROL TESTING

TC-AC-01: Default Credential Verification

Objective: Ensure no default credentials remain active.

Pre-condition: Device in factory default state.

Test Steps:

1. Attempt login using OEM default username/password.
2. Attempt login using common credentials (admin/admin, root/root, etc.).
3. Attempt login after commissioning reset.

Expected Result:

- Default credentials shall not permit access.
- System shall enforce password change on first login.

Pass Criteria: Unauthorized login attempts fail.

TC-AC-02: Role-Based Access Control (RBAC)

Objective: Validate privilege separation.

Test Steps:

1. Create roles: Admin, Operator, Viewer.
2. Login as Viewer – attempt configuration change.
3. Login as Operator – attempt firmware update.
4. Login as Admin – verify full privileges.

Expected Result:

- Viewer cannot modify configuration.
- Operator cannot upload firmware.
- Admin has full authorized privileges.

Pass Criteria: Privilege enforcement works correctly.

TC-AC-03: Account Lockout Policy

Test Steps:

1. Enter incorrect password 5 times consecutively.
2. Observe lockout behaviour.

Expected Result:

- Account locked after defined failed attempts.
- Lockout duration as per policy.

SECTION B – AUTHENTICATION & REMOTE ACCESS

TC-AUTH-01: Secure Remote Login

Applicable to: RTU / Protection Relay

Test Steps:

1. Attempt Telnet access (if IP-based).
2. Attempt SSH access.
3. Verify HTTPS availability (if web interface).

Expected Result:

- Telnet disabled.
- Only secure protocols enabled (SSH/HTTPS).
- Weak ciphers disabled.

TC-AUTH-02: Multi-Factor Authentication (Where Applicable)

Test Steps:

1. Initiate VPN access.
2. Validate OTP/token-based authentication.
3. Attempt bypass of second factor.

Expected Result:

- MFA enforced.
- Access denied without second factor.

SECTION C – PROTOCOL SECURITY TESTING

TC-PS-01: MODBUS Write Command Injection

Applicable to: RMU / MFM.

Test Steps:

1. Capture MODBUS traffic.
2. Inject unauthorized write command.
3. Observe device response.

Expected Result:

- Unauthorized command rejected OR
- Command blocked at gateway/firewall.

TC-PS-02: DNP3 Secure Authentication Validation

Applicable to: RTU

Test Steps:

1. Send authenticated control command.
2. Send unauthenticated control command.
3. Replay previous valid packet.

Expected Result:

- Only authenticated command executed.
- Replay attempt rejected.

TC-PS-03: IEC 60870-5-104 TLS Validation

Test Steps:

1. Verify TLS handshake.
2. Validate certificate chain.
3. Attempt MITM simulation.

Expected Result:

- TLS encryption active.
- Invalid certificate rejected.
- MITM attempt fails.

SECTION D – FIRMWARE SECURITY

TC-FW-01: Firmware Integrity Check

Test Steps:

1. Upload digitally signed firmware.
2. Attempt upload of tampered firmware.
3. Attempt downgrade to older version.

Expected Result:

- Only signed firmware accepted.
- Tampered firmware rejected.
- Downgrade prevented unless authorized.

SECTION E – PORT & SERVICE HARDENING

TC-PSH-01: Port Scanning

Test Steps:

1. Perform NMAP scan.
2. Identify open ports.
3. Compare with approved baseline.

Expected Result:

- Only required ports open.
- No unnecessary services running.

SECTION F – LOGGING & MONITORING

TC-LOG-01: Login Event Logging

Test Steps:

1. Perform successful login.
2. Perform failed login attempt.

3. Export logs.

Expected Result:

- Both events recorded.
- Logs contain timestamp and user ID.

TC-LOG-02: Configuration Change Logging

Test Steps:

1. Modify configuration parameter.
2. Verify audit trail entry.

Expected Result:

- Change recorded with timestamp and user ID.

SECTION G – VULNERABILITY ASSESSMENT

TC-VAPT-01: Authenticated Scan

Test Steps:

1. Perform vulnerability scan with credentials.
2. Document findings.

Acceptance Criteria:

- No Critical vulnerabilities.
- High vulnerabilities remediated prior to commissioning.

TC-VAPT-02: Unauthenticated Scan

Expected Result:

- No externally exploitable critical findings.